Testimony of Chris Klaus

I. Introduction.

I'm here today representing my company, Internet Security Systems, and also ITAA (the Information Technology Association of America) to provide you with some background information and recommendations regarding the computer security threat. Every day, Internet Security Systems stops criminal hackers and cyber-thieves by addressing vulnerabilities in computers. These individuals use the Internet for business-to-business warfare, for international cyber-terrorism, or to cause havoc and mayhem in our technology infrastructure. Internet Security Systems is involved in every aspect of computer security, whether in making the security products or in managing them. We also monitor networks and systems around the clock (24 x 7 x 365) from the US, Japan, South America, and Europe in our Security Operations Centers. We search for attacks and misuse, identify and prioritize security risks, and generate reports explaining the security risks and what can be done to fix them. At the heart of our solution is our team of world-class security experts focused on uncovering and protecting against the latest threats. This team of 200 global specialists, dubbed the X-Force, understands exactly how to transform the complex technical challenges into an effective, practical, and affordable strategy. Because of all of these capabilities, companies and governments turn to us as their trusted computer security advisor.

ITAA represents over 500 corporate member companies in the U.S., companies that build IT solutions for customers in industry and government. ITAA is a national leadership organization in the InfoSec area.

Over the years, I have watched computer vulnerabilities increase dramatically. The Internet is so useful for the very reasons that it is so vulnerable. To give you an idea of what we

are dealing with, I'd like to share an analogy. I'll compare a computer to a house. Every computer connected to the Internet has the equivalent of 65,536 doors and windows which need to be locked and monitored to make sure no one breaks in. Multiply 65,536 by every computer in every company or household and you begin to see the extent of the problem. Just as physical security companies like ADT monitor your physical doors and windows, computer security companies must lock and monitor the doors and windows of computers.

II. Example of denial-of-service attack.

A denial-of-service attack, or "DoS", is a specific type of attack on a network that is designed to bring the network to its knees. A DoS causes a network to have zero accessibility by flooding it with useless Internet traffic and requests. Many DoS attacks exploit limitations in the network. During a distributed DoS attack, a hacker actually takes over multiple computers with a "zombie" program and then, from a remote location, sets them to launch an attack all at once. This attack makes it nearly impossible to trace the hacker since the attacks appear to have come from the infected computers - which could be anywhere, such as universities, the Federal Government, businesses, or your home. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being created by hackers. Last week’s well-publicized Code Red email worm is an example of how a new DoS attack can be launched.

Code Red was designed to launch a DoS attack that would effectively shut down the White House's Web site last Thursday evening. Code Red took advantage of systems running commonly used software. Due to Code Red, more than 200,000 servers were infected to act as "zombies" that would wake up and flood the White House Web site with DoS traffic in order to force the site to shut down.

The White House was fortunate and acted in time -- in cooperation with industry -- to side-step this attack, but Code Red has forced network and system administrators to spend hours installing and testing a patch for the infected servers. And some servers may remain infected, setting the stage for possible future attacks.

III. NIPC Discussion.

I'm here to represent industry's viewpoint on the General Accounting Office (GAO) report entitled "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities". As you know, this report examines NIPC (National Infrastructure Protection Center) and recommends how NIPC can improve its ability to combat cybercrime and cyberterrorism. Before getting to the details of my findings and recommendations, I would like to point out that NIPC has made great strides. Ron Dick has been an effective leader and should be commended for his efforts in a very complicated job.

The GAO report had three main themes: 1) NIPC's limited analysis and warning capabilities; 2) lack of interagency cooperation at NIPC; and 3) reluctance of private companies to share information about cyberattacks with NIPC.

The GAO found that NIPC's analysis and warning capabilities were limited. It is our experience that the NIPC has excellent sources of information from law enforcement and intelligence sources. While we understand that some information cannot be shared due to its sensitive or classified nature, the NIPC makes every effort to craft its information into meaningful warning messages suitable for distribution to the widest possible audience.

Industry needs information as quickly as possible. However, we understand that NIPC puts a premium on accuracy in its warning products because it speaks for the federal government. Having worked with NIPC on warning products, we have seen this first

hand. While obviously not all information can be provided to the private sector, in our experience NIPC shares a broad array of information with the private sector so it can be pondered and analyzed.

Because both speed and accuracy are important, NIPC should explore ways to improve the warning process so that it can put out the most accurate warning products it can in the fastest possible time.

GAO also pointed out that the reluctance of private companies to share information about cyberattacks was an issue in the effectiveness of NIPC. We agree that NIPC would be more effective if the private sector shared more information with it, but we have seen great strides in information sharing over the past couple of years. The private sector not only runs private communications facilities, but also runs most of the Government communications facilities. We think that the ISACs (Information Sharing and Analysis Centers) and other information sharing mechanisms are a good mechanism for this information sharing to take place. However, the ISACs and other information sharing mechanisms need time to further develop. We at ISS are very supportive of ISACs and are doing our part to make this initiative as effective as possible.

We also support GAO's praise of Infraguard. Infraguard is an effective initiative. Infraguard is able to effectively get information out to the business and academic communities horizontally.

V. Information sharing is the key.

All of the above themes involve more information sharing. We have discussed how the Federal Government could be better at sharing information. Companies also could be better at sharing information. However, sharing information about corporate information security practices is inherently difficult. Companies are understandably reluctant to share sensitive

proprietary information about prevention practices, intrusions, and actual crimes with either competitors or Government agencies. No company wants information to surface that they have given in confidence that may jeopardize their market position, strategies, customer base, or capital investments.

Allowing the ISACs time to develop and grow is one way the Government can help private companies become more amenable to sharing information. The voluntary nature of ISACs or information sharing bodies is extremely important. Attempting to force this to happen would be a disaster. As I mentioned earlier in my testimony, speed is extremely important for security information to be most useful. Placing burdensome requirements on companies would cause information sharing to be a legal and time-consuming process.

To help encourage growth of the ISACs, it is important to support legislation that will strengthen information sharing legal protections that shield U.S. critical infrastructures from cyber and physical attacks and threats. Legislation that will clarify and strengthen existing Freedom of Information Act and anti-trust exemptions, or otherwise create new means to promote critical infrastructure protection and assurance, would be very helpful. This legislation would likely have a catalytic effect on the initiatives that are currently under way. It is absolutely vital that we work collectively to remove barriers to information sharing. A broad industry coalition has been working with Senator Bennett and Senator Kyl on legislation in the Senate, and with Congressman Davis and Congressman Moran in the House. On behalf of ITAA, I want to express industry support for these bills.

VI. Conclusion.

We are pleased that the Government is interested in taking computer security seriously. The United States Government spends billions of dollars buying weapons and gaining intelligence to

protect our country from more conventional types of attack. Our computer systems must also be adequately protected, or our entire infrastructure could be compromised by one person with one computer. Even though the task is complicated, computer systems can be protected.

The Government has taken great strides in the past few years. However, much, much more is needed. As industry has considerable resources and expertise, a continued partnership with industry is crucial. In addition, computer security must be a priority, and leadership and coordination are necessary in the Government. International leadership is also required. Perhaps most importantly, funding for secure Government systems must be increased by a substantial amount, and outsourcing should be considered as a viable, cost-effective option. The Government often does well with the resources it has been given. However, computer security specialists are required to implement and coordinate many different security products and services to adequately secure a system. As computer security expertise is extremely rare, the cost of computer security specialists is astronomical. To help address the cost of computer security, educational efforts must be undertaken to train the personnel required.

Thank you for inviting me here today. I look forward to a continuing dialog on the computer security issue, and hope that, working together, we can adequately secure our country's assets and information.